# Microsoft DevOps Solutions: Designing an Authentication and Authorization Strategy

#### AZURE AUTHENTICATION AND AUTHORIZATION



John Savill
PRINCIPAL CLOUD SOLUTION ARCHITECT
@NTFAQGuy www.savilltech.com

# Learning Objectives



Design an access solution (Azure AD Privileged Identity Management (PIM), Azure AD Conditional Access, MFA)

Organize the team using Azure AD groups

Implement Service Principals and Managed Identity

**Configure service connections** 



# Module Overview



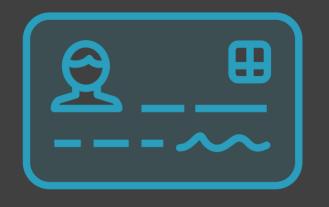
Azure AD authentication

**Authorization with Conditional Access** 

Using groups with Azure AD

Role-based access control in Azure





Identity is key to not only application execution but DevOps functionality.



Understanding the authentication and authorization options for applications and DevOps is critical.

## Azure Active Directory Refresher

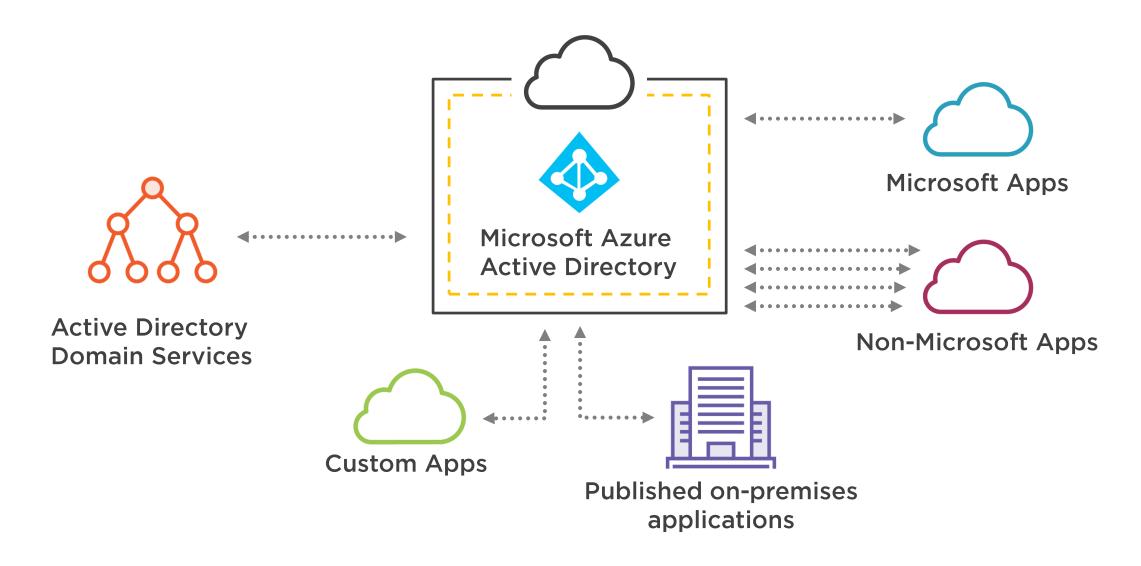
Azure Active Directory (AD) is an enterprise identity provider

Globally available from virtually any device

Utilizes a flat structure allowing users, groups and other objects to be created

Cloud authentication protocols instead of Kerberos, NTLM (by default)

# Azure AD High Level View



#### Azure AD Authentication Methods



Cloud authentication with password hash



Pass-through authentication



**Federation** 

#### MFA



Passwords are a network secret

Once known it can be used anywhere

Focus is to use multiple factors for authentication (MFA)

- Something I know (e.g. a password or pin)
- Something I have (e.g. a phone or laptop)
- Something I am (e.g. biometrics)

Therefore pins and biometrics with Windows Hello are attractive as its local ONLY to a specific machine

#### Azure AD MFA



#### Utilizes the user's phone via

Call

Text

Authenticator app via a code or approval of notification

#### Conditional Access



Conditional access focused on authorization but can force strong authentication, i.e. require MFA

A P1 feature with P2 required for user risk integration

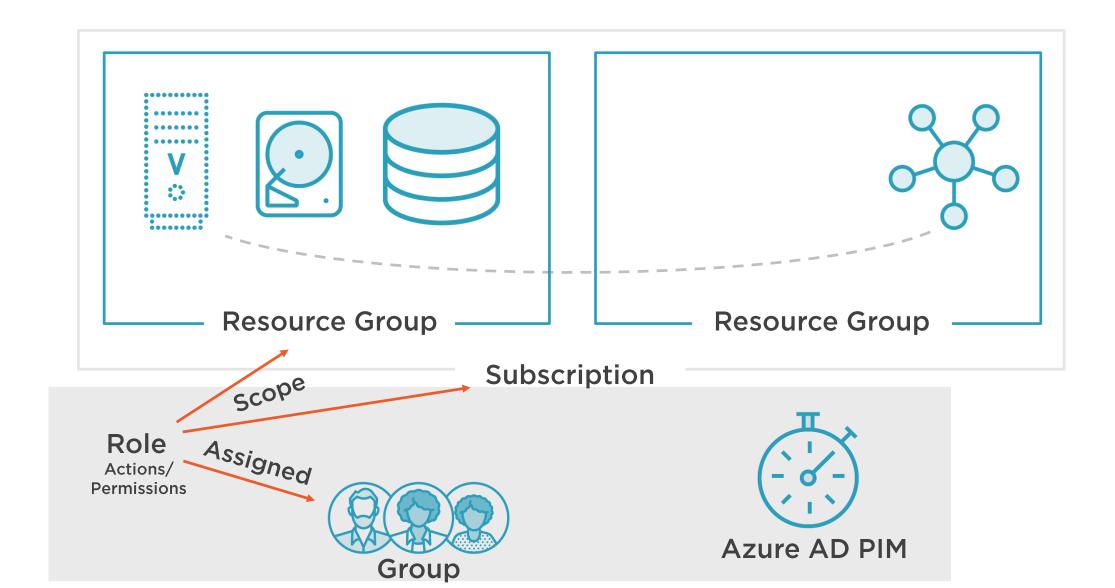
Enables a set of conditions to be specified

When the conditions are met the controls specified are enforced

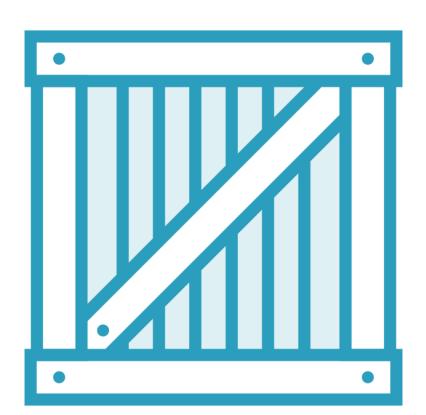
Attributes such as location, device health, which application is being accessed, user risk and more can be used as part of policies

These apply for all types of identity which means consider this for service principals to ensure access it not unintentionally blocked

#### Role-Based Access Control



# Azure Roles



Large number of built-in roles

Three core roles apply to all resource types

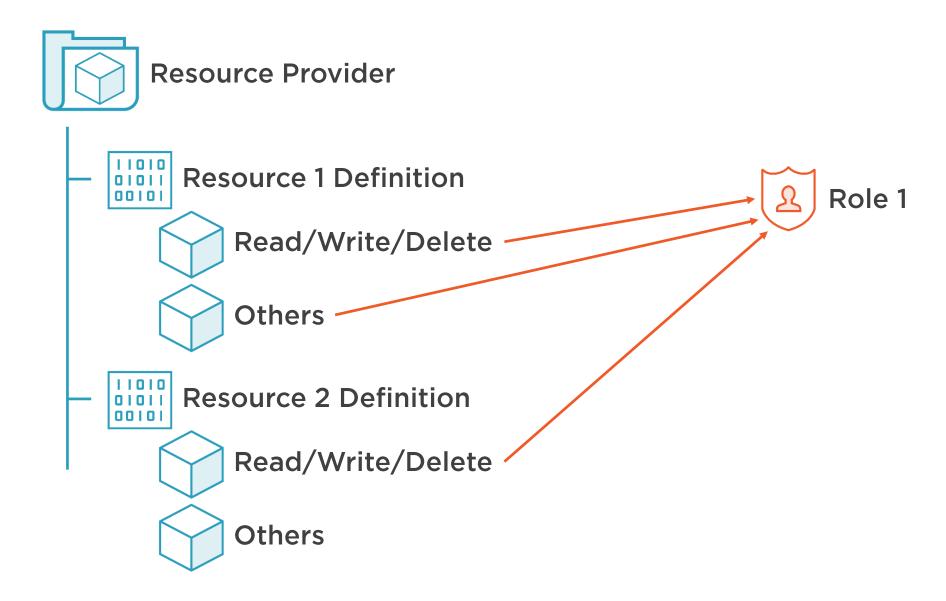
- Owner
- Contributor
- Reader

Other roles are specific to certain types of Azure resource

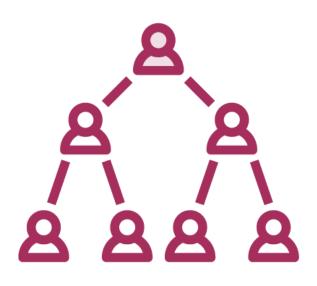
Focus on assigning permissions to groups rather than directly to users

Permissions are inherited

#### Role Structure



#### Azure AD Roles



Azure AD is a flat structure

Roles are Azure AD wide

Administrative Units allow scoping supported by some roles

Custom roles are possible but currently in preview

To assign role to a group, special cloud group must be used

## Role Assignment



Preferred model is assigning roles to groups and add users to group

The group is granted the role at a specific scope

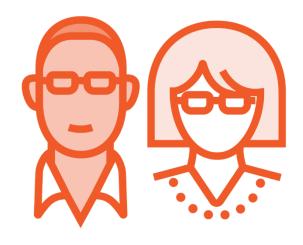
Users are added and removed from the group and will gain the role

## Groups in Azure AD



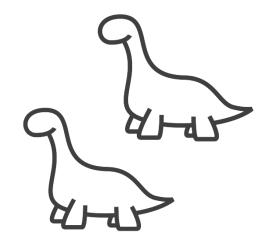
# Azure AD Security Groups

Security principal
Cloud or sync'd
Static or dynamic
Cloud group for AAD roles



Microsoft 365 Groups

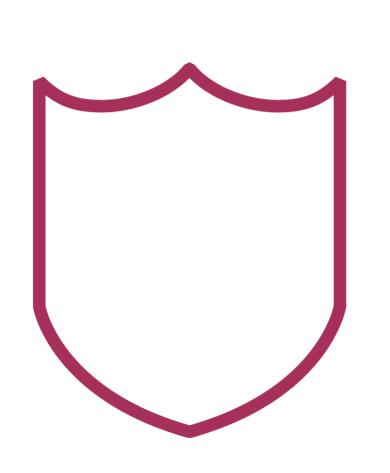
Provides access to Microsoft 365 resources



**SharePoint Groups** 

Allow permissions to be give to SharePoint resources only

## Privileged Identity Management



A P2 feature

**Enable just-in-time elevation** 

Instead of users having roles assigned to them (for Azure AD, Azure ARM and Office 365) permanently the right to elevate to roles is assigned

Users can then elevate for a fixed duration after potentially additional authentication, e.g. MFA

Integration with ticketing and approval available

### Summary



**Azure AD authentication** 

**Authorization with Conditional Access** 

Using groups with Azure AD

Role-based access control in Azure



# Next Up: Azure AD Application and DevOps Integration

